IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF ALABAMA SOUTHERN DIVISION

BARRON PARTRIDGE, individually and on behalf of all other residents of the State of Alabama similarly situated,

Plaintiff,

CIVIL ACTION NO.: 1:17-cv-423

v.

EQUIFAX, INC.,

Defendant.

CLASS ACTION COMPLAINT

Plaintiff Barron Partridge ("Plaintiff") brings the following Complaint, individually and on behalf of all other residents of the State of Alabama similarly situated, against the Defendant Equifax, Inc. ("Equifax"):

NATURE OF THE CASE

1. Plaintiff brings this class-action case against Defendant Equifax for its failure to secure and safeguard consumers' personally identifiable information ("PII") which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency.

2. Equifax has acknowledged the occurrence of a cybersecurity incident ("the Data Breach") potentially impacting approximately 143 million U.S. consumers. It has acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax represents that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information accessed includes names, Social Security numbers, birthdates, addresses,

and, in some instances, driver's license numbers. In addition, Equifax has admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with PII for approximately 182,000 U.S. consumers, were accessed.

PARTIES, JURISDICTION, AND VENUE

3. Plaintiff Barron Partridge is a resident citizen of Mobile County, Alabama.

4. Defendant Equifax, Inc., is a corporation organized under the laws of the State of Delaware with its principal place of business located in Atlanta, Georgia.

5. This Court has subject-matter jurisdiction of this class action pursuant to 28 U.S.C. § 1332(d)(2)(A). The matter in controversy, the aggregated claims of the individual class members, exceeds the sum of $5 million, exclusive of interest and costs; there are more than 100 members in the proposed class; and all members of the proposed class, including Plaintiff, are citizens of a State different from Equifax. Plaintiff and the members of the proposed class are all citizens of the State of Alabama.

6. This Court has personal jurisdiction over Equifax for the following reasons. Equifax is in the business of assembling consumer credit information it regularly obtains from within this State and from within this judicial district, and that it regularly sells to others within this State and within this judicial district. Plaintiff's claims against Equifax are for Equifax's failure to safeguard Plaintiff's PII in his consumer credit information it acquired and sold within this State and within this judicial district. Therefore, Plaintiff's claims arise out of or relate to Equifax's purposeful contacts with this State and with this judicial district.

7. Venue is proper in the Southern District of Alabama pursuant to 28 U.S.C. § 1391(b)(1) and (d). Equifax is subject to personal jurisdiction in this State and in this

judicial district, for the reasons explained in the preceding paragraph, and therefore Equifax, the only Defendant in this action, resides in this judicial district.

FACTUAL BACKGROUND

8. Equifax is one of three nationwide credit-reporting companies that track and rate the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments, and credit cards, as well as information on such things as child-support payments, credit limits, missed rent and utilities payments, addresses, and employer history. All this information, and more, factors into credit scores.

9. Unlike most data breaches, not all of the people affected by the Equifax Data Breach may be aware that the company has their PII. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

10. According to Equifax's report on September 7, 2017, the Data Breach was discovered on July 29th. The perpetrators gained access by "[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to retrieve "certain files."

11. Included among those files was a treasure trove of personal data: names, dates of birth, Social Security numbers, and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.

12. Personal data like this is a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

13. Plaintiff has suffered actual injury because his PII was improperly disclosed and accessed by cybercriminals in the Data Breach.

14. Plaintiff has suffered actual injury because his PII has already been misused by criminals, as set out subsequently herein.

15. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII – a form of intangible property that was compromised in and as a result of the Data Breach.

16. Additionally, Plaintiff is exposed to imminent and impending injury arising from the virtually certain occurrence of future fraud, identity theft, and PII misuse due to his PII being placed in the hands of criminals.

17. At all relevant times, Equifax was well aware, or reasonably should have been aware, that the PII collected, maintained, and stored in its systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

18. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiff and the Class members.

19. PII is a valuable commodity because it contains not only payment-card numbers but personal identifiers as well. A “cyber black market” exists in which criminals openly post stolen payment-card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is extremely valuable to identity thieves because they can use victims’ personal data to open new financial

accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

20. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches ... not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[1]

21. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including the significant costs that would be imposed on individuals as a result of a breach.

22. Equifax was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Equifax's systems.

23. Nonetheless, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the PII of Plaintiff and the Class members was wanton, reckless, or at the very least, negligent.

24. The ramifications of Equifax's failure to keep Plaintiff's and the Class members' data secure are severe.

[1] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci201 4.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 10, 2017).

25. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[3]

26. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

27. Identity thieves can use personal information, such as that of Plaintiff and the Class members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

28. Javelin Strategy and Research reports that identity thieves have stolen

---

[2] 17 C.F.R. § 248.201 (2013).

[3] *Id.*

[4] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft(last visited April 10, 2017).

$112 billion in the past six years.[5]

29. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity-theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

30. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

31. Plaintiff and the Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent

---

[5] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).

[6] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).

[7] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

use of their PII.

32. The PII of Plaintiff and the Class members is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain Plaintiff's and the Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

33. The Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and the Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class members' PII and to protect against reasonably foreseeable threats to the security or integrity of such information.

34. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

35. Had Equifax remedied the deficiencies in its data-security systems, followed security guidelines, adopted security measures recommended by experts in the field, and otherwise exercised reasonable care, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

36. Equifax's wrongful actions and inactions directly and proximately caused the theft and dissemination to unauthorized third parties of Plaintiff's and the Class members' PII, causing them to suffer, and continue to suffer, some or all of the following

damages for which they are entitled to compensation:

a. Their PII was improperly disclosed and accessed by cybercriminals in the Data Breach;

b. Theft of their personal and financial information;

c. Unauthorized charges on their debit and credit card accounts;

d. Other actual misuse of their PII including fraud and identity theft;

e. Imminent and impending injury arising from the virtually certain occurrence of future fraud, identity theft, and PII misuse due to their PII being placed in the hands of criminals;

f. Loss of privacy;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

i. Imminent and impending ascertainable losses in the form of the loss of cash-back or other benefits as a result of inability to use certain accounts and cards affected by the Data Breach;

j. Imminent and impending loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees; and

k. Adverse effects on their credit including decreased credit scores and adverse credit notations.

THE FACTS PERTAINING TO THE NAMED PLAINTIFF

37. Plaintiff's PII was disclosed and accessed by unauthorized persons during the Data Breach.

38. Beginning in late May, 2017, there have been thirteen attempts by

unauthorized persons to open credit cards in Plaintiff's name.

39. In August 2017, an unauthorized person opened a credit card in Plaintiff's name with Credit One Bank, located in Las Vegas, Nevada. Plaintiff discovered that the unauthorized credit card had been opened and had it closed.

40. Prior to these occurrences, Plaintiff had never suffered any incidents of identity theft.

CLASS-ACTION ALLEGATIONS

40. Plaintiff seeks relief on behalf of himself and all others in the State of Alabama who are similarly situated. Pursuant to Fed.R.Civ.P. 23(a) and (b)(3), Plaintiff seeks certification of a class defined as follows:

> All persons residing in the State of Alabama whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.
>
> Excluded from the Class are (1) all employees of Equifax and any of its affiliates, parents or subsidiaries; and (2) all judicial officers of the United States who preside over or hear this case, and all persons related to them as specified in 28 U.S.C. § 455(b)(5).

41. The members of the Class are readily identifiable from the information and records in the possession or control of Equifax.

42. Upon information and belief, the Class consists of thousands of individual members, and is therefore so numerous that individual joinder of all members is impracticable. The members of the Class are geographically dispersed throughout the State of Alabama.

43. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual members of the Class. The

questions common to the Class include, but are not limited to, the following:

a. Whether Equifax had a duty to protect PII;

b. Whether Equifax knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Equifax's security measures for the protection of its systems were reasonable and adequate;

d. Whether Equifax was negligent with respect to its security measures;

e. Whether Equifax's security measures allowed the Data Breach to occur;

f. Whether Equifax's conduct, including its failure to act, was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and the Class members; and

g. Whether Plaintiff and the Class members were injured and suffered damages because of Equifax's failure to reasonably protect its systems and data network.

44. Plaintiff's claims are typical of those of the Class, and are based on the same legal theories as those of the Class members. Plaintiff had his PII compromised in the Data Breach. Plaintiff's damages and injuries are akin to those of other Class members and Plaintiff seeks relief consistent with the relief sought by the Class.

45. Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained counsel who are highly experienced and competent in complex consumer class-action litigation, and Plaintiff and his counsel intend to prosecute this action vigorously. Neither Plaintiff nor his counsel have any interests that might cause them not to vigorously pursue this action. Plaintiff's interests are coextensive with those of the Class, and Plaintiff has no interests adverse to those of the Class members.

46. Plaintiff has made arrangements with his counsel for the discharge of his financial responsibilities to the Class members. Plaintiff's counsel have the necessary

financial resources to adequately and vigorously litigate this class action.

47. A class action is superior to all other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this case as a class action. It is desirable to concentrate the litigation of the claims in this forum, because the damages suffered by the individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Equifax. Thus, it is unlikely that the Class members, on an individual basis, can obtain effective redress for the wrongs done to them. For these reasons, the Class members' interests in individually controlling the prosecution of separate actions are minimal. Additionally, the court system would be adversely affected by such individualized litigation. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase delay and expense to all parties and the court system from the issues raised by this action. In contrast, the class-action device provides the benefit of adjudication of these issues in a single proceeding, with economics of scale and comprehensive supervision by a single court.

48. Plaintiff and his counsel are aware of several putative national class actions arising out of the Data Breach filed by citizens of other States in other States. Plaintiff and his counsel are also aware of three putative national class actions arising out of the Data Breach filed by citizens of this State in the Northern District of Alabama. Plaintiff and his counsel are, however, aware of no litigation concerning the controversy already begun by Class members on an Alabama-only class basis.

COUNT I
NEGLIGENCE

49. Plaintiff realleges Paragraphs 1 through 48 as if fully set forth herein.

50. Upon accepting and storing the PII of Plaintiff and the Class members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff and the Class members to exercise reasonable care to secure and safeguard that information and to use reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

51. Equifax owed a duty of care not to subject Plaintiff and the Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

52. Equifax owed a duty to Plaintiff and to the members of the Class to exercise reasonable care in retaining, securing, safeguarding, and protecting PII in its possession, and to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices.

53. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

54. Equifax knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and the Class members' PII.

55. Equifax breached its duties to Plaintiff and the Class members in various ways, including:

a. By failing to provide reasonable and adequate data-security

measures to safeguard the PII of Plaintiff and the Class members;

b. By failing to install reasonable and adequate firewalls and barriers to prevent unauthorized intrusion into its data systems and networks;

c. By failing to implement reasonable and adequate security protocols and procedures to protect Plaintiff's and the Class members' PII, including but not limited to system and event monitoring;

d. By not taking timely and appropriate measures to patch its website vulnerability when it knew or should have known of the vulnerability, and when such measures were readily available to Equifax; and

e. By failing to comply with minimum data-security industry standards during the period of the Data Breach.

56. As a direct and proximate result of Equifax's negligence, Plaintiff and the Class members were damaged as specified in Paragraph 36 hereof.

COUNT II
WANTONNESS

57. Plaintiff realleges Paragraphs 1 through 48 as if fully set forth herein.

58. Equifax knew Plaintiff and the Class members would be probable victims of any inadequate data-security practices. Equifax knew of the importance of adequate security.

59. Equifax has had many data breaches in the past, and its former employees have stated that its data-security practices have deteriorated in recent years.

60. Equifax knew that its data systems and networks did not adequately safeguard Plaintiff's and the Class members' PII.

61. Equifax knew that if Plaintiff's and the Class members' PII was accessed by unauthorized third parties, Plaintiff and the Class members would likely or probably suffer the damages previously specified in Paragraph 36 hereof.

62. Equifax, with knowledge of the existing conditions and being conscious that

injury to Plaintiff and the Class members would likely or probably result from its conduct, was wanton in one or more of the following respects:

a. By failing to provide reasonable and adequate data-security measures to safeguard the PII of Plaintiff and the Class members;

b. By failing to install reasonable and adequate firewalls and barriers to prevent unauthorized intrusion into its data systems and networks;

c. By failing to implement reasonable and adequate security protocols and procedures to protect Plaintiff's and the Class members' PII, including but not limited to system and event monitoring;

d. By not taking timely and appropriate measures to patch its website vulnerability when it knew of the vulnerability, and when such measures were readily available to Equifax; and

e. By failing to comply with minimum data-security industry standards during the period of the Data Breach.

63. As a direct and proximate result of Equifax's wantonness, Plaintiff and the Class members were damaged as specified in Paragraph 36 hereof, and are entitled to recover punitive damages as well as compensatory damages.

COUNT III
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")

64. Plaintiff realleges Paragraphs 1 through 48 as if fully set forth herein.

65. As individuals, Plaintiff and the Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

66. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties ...." 15 U.S.C. § 1681a(f).

67. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

68. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to ... limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

69. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for – (A) credit ... to be used primarily for personal, family, or household purposes; ... or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

70. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit

reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

71. Equifax furnished the Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; and knowingly or recklessly failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

72. Equifax knowingly or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The knowing or reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willfully failed to take them.

73. Equifax also acted knowingly or recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the FTC. *See e.g.,* 55 Fed.Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600,

Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knowns or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and in depriving Plaintiff and other members of the classes of their rights under the FCRA.

74. Equifax's knowing or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and the Class members' personal information for no permissible purposes under the FCRA.

75. Plaintiff and the Class members have been damaged by Equifax's knowing or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

76. Plaintiff and the Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT IV
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

77. Plaintiff realleges Paragraphs 1 through 48 as if fully set forth herein.

78. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data

breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

79. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the Class members' PII and consumer reports for no permissible purposes under the FCRA.

80. Plaintiff and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

81. Plaintiff and the Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all members of the proposed Class, asks that the Court:

a. Certify the Class, as defined herein;

b. Appoint Plaintiff as representative of the Class;

c. Appoint Plaintiff's counsel as attorneys for the Class;

d. Enter judgment awarding Plaintiff and the Class members monetary damages, as allowed by law, in an amount to be determined;

e. Award Plaintiff and the Class members a reasonable attorneys' fee and costs; and

f. Provide such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and the Class members, demands a trial by jury on all

issues so triable.

Respectfully submitted this 20th day of September, 2017.

TAYLOR MARTINO, P.C.

By: /s/ *Steven A. Martino*

STEVEN A. MARTINO (MARS7433)
W. LLOYD COPELAND (COPW3831)
W. BRADFORD KITTRELL (KITW3444)
KENNETH A. METZGER (METK4856)
P.O. Box 894
Mobile, Alabama 36601
Telephone: (251) 433-3131
Facsimile: (251) 405-5080
E-Mail: stevemartino@taylormartino.com
lloyd@taylormartino.com
bkittrell@taylormartino.com
kenny@taylormartino.com
ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS

LAW OFFICES OF RICHARD R. ROSENTHAL, P.C.
RICHARD R. ROSENTHAL
Title Building
300 North Richard Arrington Jr., Blvd.
Suite 200
Birmingham, Alabama 35203
Telephone: (205) 533-9909
E-Mail: rosenthallaw@bellsouth.net
ATTORNEY FOR PLAINTIFF AND THE PROPOSED CLASS

DEFENDANT TO BE SERVED:

Equifax, Inc.
c/o Prentice Hall Corporation System Inc.
641 South Lawrence Street
Montgomery, Alabama 36104

Via Certified Mail by Clerk